Department of Health & Human Services
Public Key Infrastructure (PKI) Program

Public Trust TLS Certificate Request Procedures

Version 1.0 - DRAFT

July 2013

1. Document Purpose & Scope

1.1 Purpose

This document is intended to provide an overview of HHS’s PKI Program’s Transport Layer Security (TLS) certificate offerings and to explain the steps for processing a Certificate Signing Request (CSR) with the Entrust Certificate Authority.

1.2 Audience

There are three roles identified with the Public Trust TLS CSR process:

- **System Owners/Administrators** – are responsible for a system’s (web server, database service) day-to-day operations and for generating CSRs for that that system

- **Authorized Requestors** – individuals authorized by their OpDivs to request certificates on behalf of System Owners/Administrators

- **Entrust Local Registration Authorities (LRAs)** – persons trained and authorized by Entrust to approve certificate requests for the Entrust Certificate Authority (CA)

This document was written to provide Authorized Requestors, referred to as “Requestors” throughout this document with the steps and information they need to successfully process CSRs on behalf of their OpDiv System Owners/Administrators. Going forward, Requestors can initiate a Public Trust TLS CSR using the on-line data entry form as per the instructions below.

1.3 Scope

This document contains the procedures a Requestor will follow to process an HHS PKI Program’s Public Trust TLS Certificate. Common Policy processes vary slightly from the Public Trust request processes (e.g. User interface, URL etc.) and are considered out of scope for this document.

Additionally, the following information is out of scope for this document:

- Generating a CSR for a specific operating systems
- Installing a TLS certificate once it is retrieved by the requestor
- LRA training requirements and CSR approving procedures

2. HHS PKI Program's TLS Certificate Overview

2.1 Public Trust vs. Common Policy Based Certificates

The HHS PKI Program offers two different types of TLS certificates: Public Trust and Common Policy. The attributes of each type of TLS certificate is provided in the table below.

PUBLIC TRUST	COMMON POLICY
Also called "External TLS certificates" at HHS	Also called "Internal TLS certificates" at HHS
Trusted root CA is: **Entrust.net Certification Authority (2048)**	Trusted root is: **Entrust Managed Services Root CA**
Trusted root CA is widely distributed via the major internet browser vendors	Trusted root CA certificate must be distributed to relying parties and manually installed
Not cross-certified with the Federal Common Policy CA	Cross-certified with the **Federal Common Policy CA**

**Note: Instructions for Common Policy processes and procedures will be included as part of a separate user guide.*

In general, if a system or web server is going to be accessed by HHS / OpDiv users only, an Internal/ Common Policy TLS certificate is recommended. Because Common Policy TLS certificates are issued by HHS's own CA, the certificates are significantly less expensive than the Public Trust TLS certificates.

However, if a system or web server is going to be accessed by users or other systems external to HHS, then a Public Trust TLS certificate is recommended.

3. HHS PKI Program Public Trust Certificate Request Procedures

3.1 Overview

The overall steps a Requestor will follow to process a CSR are as follows:

1. Create a TLS certificate request in the Entrust Certificate Management System (CMS)
2. Submit the request to an LRA for approval
3. Retrieve the certificate.

The remainder of this document explains in detail how to execute each of these steps.

3.2 Procedure for Requesting a Public Trust Certificate

Follow these steps for requesting Public Trust certificate.

3.2.1 Requesting and Receiving the Authorization and Reference Codes

The HHS Common Policy TLS CSR process begins with the Requestor sending an email to the HHS PKI Helpdesk. If approved, the email request will result in the receipt of two emails, each containing one piece of the Activation Code. One email will be received from the HHS PKI Helpdesk and the other email will be automatically generated by the Entrust HHS Enrollment Server for Web application. A Requestor will require both codes (Authorization code and Reference code) to generate a certificate request.

Step 1:

Send an email to the HHS PKI Helpdesk (USHHSPKIHelpdesk@deloitte.com) containing the following information:

- The Common Name (CN) for the system/application requiring a certificate
- The Email address of the Authorized requestor.
  Note: This email address will be used by the Entrust **HHS Enrollment Server for Web** application to send the Reference Code and will also be used to contact system administrators if and when Entrust notifications or certificate expiration notifications are required to be sent.

3.2.2 Create an TLS Certificate Request using e-Form

Note: Only CSR's received from Authorized Requestors will be approved by the LRA.

Step 1:

Navigate to the following URL using an internet browser:
(https://www.entrust.net/webhost/index.cfm?code=1-1M6GQM&validationcode=0F606031-09E8-7DC1-106AC4FA318683E5)

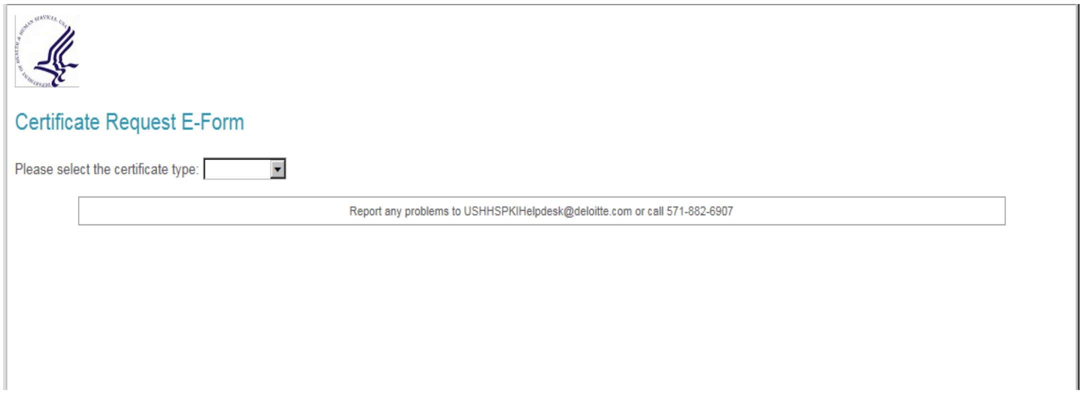
Note: Only approved requestors will be provided the password for the above URL.

The Certificate Request E-Form page appears as shown below.

Step 2:

Select the **certificate type** from the dropdown menu.

Figure 1 Certificate Request E-Form



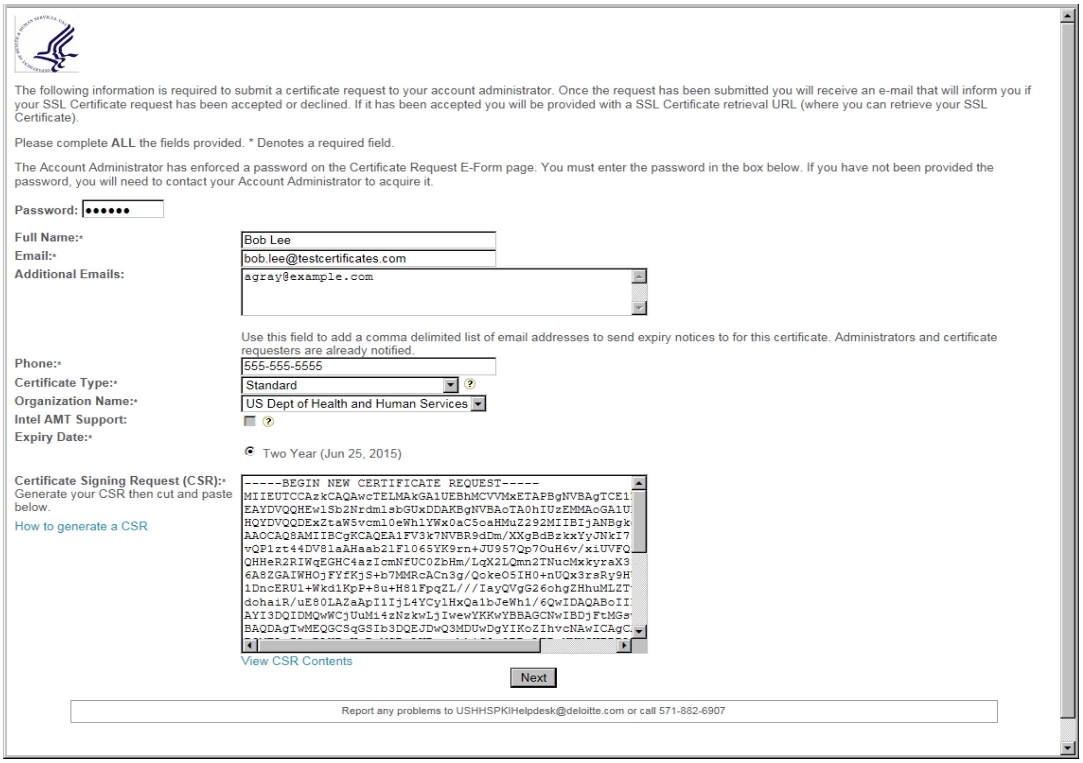
Certificate Request E-Form

Please select the certificate type:

Report any problems to USHHSPKIHelpdesk@deloitte.com or call 571-882-6907

Once the certificate type is selected, the next page of the TLS Certificate Request will appear:

Figure 2 TLS Certificate Request



The following information is required to submit a certificate request to your account administrator. Once the request has been submitted you will receive an e-mail that will inform you if your SSL Certificate request has been accepted or declined. If it has been accepted you will be provided with a SSL Certificate retrieval URL (where you can retrieve your SSL Certificate).

Please complete **ALL** the fields provided. * Denotes a required field.

The Account Administrator has enforced a password on the Certificate Request E-Form page. You must enter the password in the box below. If you have not been provided the password, you will need to contact your Account Administrator to acquire it.

Password: ••••••

Full Name:*	Bob Lee
Email:*	bob.lee@testcertificates.com
Additional Emails:	agray@example.com Use this field to add a comma delimited list of email addresses to send expiry notices to for this certificate. Administrators and certificate requesters are already notified.
Phone:*	555-555-5555
Certificate Type:*	Standard
Organization Name:*	US Dept of Health and Human Services
Intel AMT Support:	□
Expiry Date:*	● Two Year (Jun 25, 2015)

Certificate Signing Request (CSR):*
Generate your CSR then cut and paste below.
How to generate a CSR

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEUTCCAzkCAQAwcTELMAkGA1UEBhMCVVMxETAPBgNVBAgTCE1
EAYDVQQHEwlSb2NrdmlsbGUxDDAKBgNVBAoTA0hIUzEMMAoGA1U
HQYDVQQDExZtaW5vcml0eWhlYWx0aC5oaHMuZ292MIIBIjANBgk
AAOCAQ8AMIIBCgKCAQEA1FV3k7NVBR9dDm/XXgBdBzkxYyJNkI7
vQP1zt44DV8laAHaab2lFl065YK9rn+JU957Qp7OuH6v/xiUVFQ
QHHeR2RIWqEGHC4azIcmNfUC0ZbHm/LqX2LQmn2TNucMxkyraX3
6A8ZGAIWHOjFYfKjS+b7MMRcACn3g/QokeO5IH0+nUQx3rsRy9H
1DncERUl+Wkd1KpP+8u+H81FpqZL///IayQVgG26ohgZHhuMLZT
dohaiR/uE80LAZaApI1IjL4YCylHxQa1bJeWh1/6QwIDAQABoII
AYI3DQIDMQwWCjUuMi4zNzkwLjIwewYKKwYBBAGCNwIBDjFtMGs
BAQDAgTwMEQGCSqGSIb3DQEJDwQ3MDUwDgYIKoZIhvcNAwICAgC
```

View CSR Contents

Next

Report any problems to USHHSPKIHelpdesk@deloitte.com or call 571-882-6907

Step 3:

Complete the information for all the fields on the page, as follows:

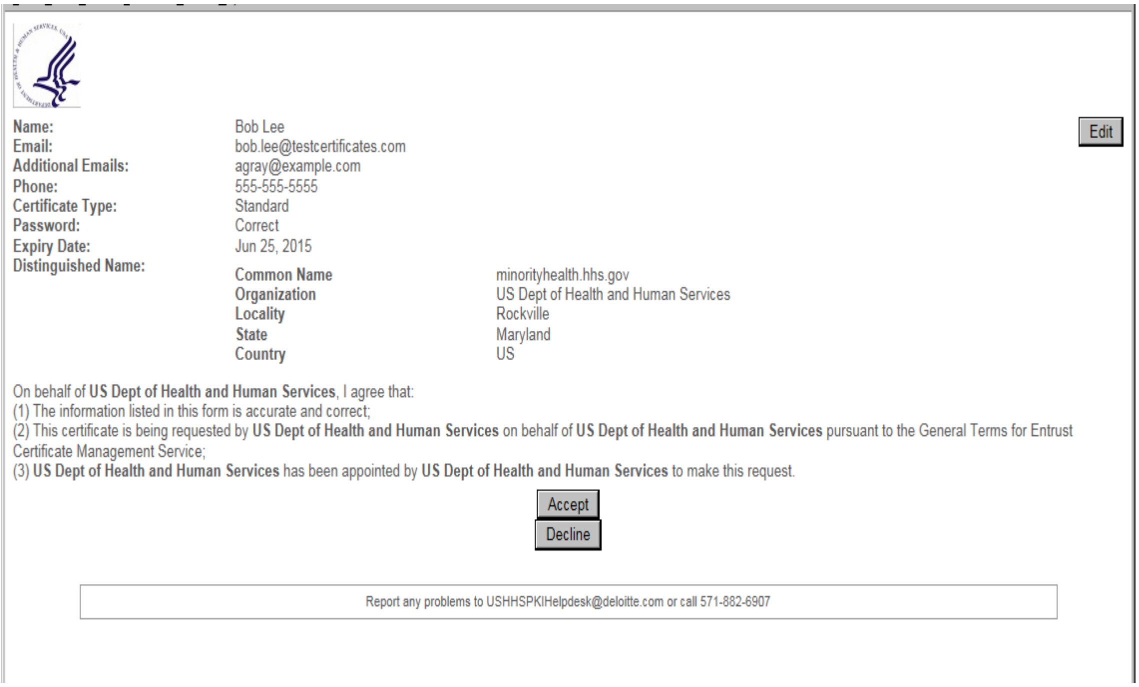
- **Password -** Enter the password, as provided to Authorized Requestors by the LRA.
- **Full Name -** Enter the full name of the Authorized Requestor.
- **Email -** Enter the email address of the Authorized Requestor.
- **Additional Emails -** Enter the additional email addresses of any persons (e.g. Server administrator's group email account) other than the Authorized Requestor who should receive expiry notifications. Separate these email addresses with commas.
- **Phone -** Enter the telephone number of the Authorized Requestor.
- **Certificate Type -** This field is filled automatically according the type of certificate requested.
- **Organization Name –** Select US Dept. of Health and Human Services from the drop-down menu.
- **Expiry Date -** Select the lifespan of the certificate. (Note: The Two year lifespan is the option available)
- **Certificate Signing Request -** Copy the certificate signing request (created on the machine where the certificate will be installed) into the field provided. Be sure to include the "***Begin new certificate request"*** and "***End new certificate request"*** statements, including the leading and trailing dashes.

Step 4:

Click **Next**.

A confirmation screen appears.

Figure 3 Confirmation Screen



Name:	Bob Lee	
Email:	bob.lee@testcertificates.com	
Additional Emails:	agray@example.com	
Phone:	555-555-5555	
Certificate Type:	Standard	
Password:	Correct	
Expiry Date:	Jun 25, 2015	
Distinguished Name:	Common Name	minorityhealth.hhs.gov
	Organization	US Dept of Health and Human Services
	Locality	Rockville
	State	Maryland
	Country	US

On behalf of **US Dept of Health and Human Services**, I agree that:
(1) The information listed in this form is accurate and correct;
(2) This certificate is being requested by **US Dept of Health and Human Services** on behalf of **US Dept of Health and Human Services** pursuant to the General Terms for Entrust Certificate Management Service;
(3) **US Dept of Health and Human Services** has been appointed by **US Dept of Health and Human Services** to make this request.

Report any problems to USHHSPKIHelpdesk@deloitte.com or call 571-882-6907

Step 5:

Review the information contained on the confirmation page (shown above). If it is correct, select **Accept**. If not, select **Decline**.
Note: If "Decline" is selected, the user will be required to start the entire process over.

3.2.3 Await LRA Approval

Upon clicking the **Accept** button, the Entrust CMS sends an email message to the LRAs notifying them that a new request requires their approval. The LRAs must approve the request before the certificate is created.

If the LRA approves the request, the Entrust CMS sends an automated email message, containing a link to retrieve the certificate, back to the Requestor.

If the LRA declines the request, an automated email message stating that the request has been declined will be sent to Requestor. The email will contain an explanation for why the request was declined.

3.2.4 Retrieve CSR

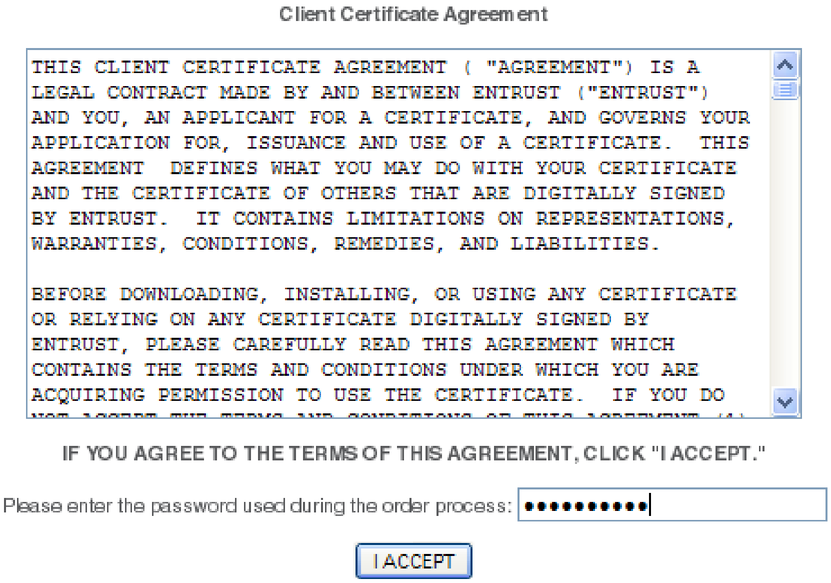
Upon approval of the CSR by the LRA, a Requestor may either follow the step below to retrieve the signed certificate themself, or they may choose to forward the email message with the retrieval link to the System Owner/Administrator. The user must perform the following actions to retrieve the signed TLS certificate:

Click the link, provided in the approval email, to open the certificate download page.

If the recipient is using Microsoft® Internet Explorer, the browser downloads and installs the certificate after they accept the license agreement on the certificate download page.

For instructions about using a different browser, please refer to the **Installation Guide** link on the Web page that appears after clicking **I Accept**.

Figure 4 Client Certificate Agreement



Client Certificate Agreement

THIS CLIENT CERTIFICATE AGREEMENT ("AGREEMENT") IS A LEGAL CONTRACT MADE BY AND BETWEEN ENTRUST ("ENTRUST") AND YOU, AN APPLICANT FOR A CERTIFICATE, AND GOVERNS YOUR APPLICATION FOR, ISSUANCE AND USE OF A CERTIFICATE. THIS AGREEMENT DEFINES WHAT YOU MAY DO WITH YOUR CERTIFICATE AND THE CERTIFICATE OF OTHERS THAT ARE DIGITALLY SIGNED BY ENTRUST. IT CONTAINS LIMITATIONS ON REPRESENTATIONS, WARRANTIES, CONDITIONS, REMEDIES, AND LIABILITIES.

BEFORE DOWNLOADING, INSTALLING, OR USING ANY CERTIFICATE OR RELYING ON ANY CERTIFICATE DIGITALLY SIGNED BY ENTRUST, PLEASE CAREFULLY READ THIS AGREEMENT WHICH CONTAINS THE TERMS AND CONDITIONS UNDER WHICH YOU ARE ACQUIRING PERMISSION TO USE THE CERTIFICATE. IF YOU DO

IF YOU AGREE TO THE TERMS OF THIS AGREEMENT, CLICK "I ACCEPT."

Please enter the password used during the order process: ••••••••••

Once the process is completed the user can close their browser.

For any additional questions regarding these HHS PKI Program Public Trust Certificate Request Procedures, or about the HHS PKI Program’s TLS Certificate offerings, please send an email with a full description of the issue and return contact information to: USHHSPKIHelpdesk@Deloitte.com.